Title: Blockchain and AI Threat Intelligence in Autonomous Transportation Networks

- Journal: *International Journal of Emerging Digital Systems*

- Author(s): *Kael Veyron*
- Affiliation: *School of Information Systems, Atlantic Research Institute*

- Domain(s):
    - Computer Science [cs]
    - Economics and Finance [q-fin]
    - Social and Information Networks [cs.SI]
- Date of publication: *September 2025*

Keywords: Autonomous Vehicles, Blockchain, Artificial Intelligence, IoT, Cybersecurity, Transportation Security, Threat Intelligence

---

Abstract
Autonomous transportation networks depend on IoT sensors, vehicle-to-vehicle (V2V) communication, and artificial intelligence for navigation and safety. These systems promise efficiency but expose public safety to cyber threats. Attacks against autonomous vehicles or connected infrastructure could cause collisions, traffic disruption, and loss of trust in self-driving technology. Traditional cybersecurity models struggle with the scale and complexity of transportation IoT. This paper examines how blockchain and AI enhance cyber threat intelligence in autonomous transportation. Blockchain provides decentralized trust and immutable event logs, while AI delivers real-time anomaly detection and predictive defense. The study reviews methodology, analyzes current deployments, and outlines a future outlook. Findings indicate that blockchain-AI convergence will be critical for safe autonomous mobility. By 2035, regulators are expected to require blockchain-backed AI threat intelligence as a baseline for transportation systems.

Methodology
The research followed a three-step evaluation:

1. **Case Study Review**: Documented cyberattacks on connected vehicles and transport systems from 2015 to 2024 were analyzed. This included remote car hijacking incidents, GPS spoofing, and attacks on smart traffic lights.
2. **Blockchain Testing**: Permissioned blockchains such as Hyperledger and Quorum were tested for V2V and vehicle-to-infrastructure (V2I) communication. Authentication latency, throughput, and scalability were measured under simulated highway traffic of 10,000 vehicles.
3. **AI Models**: Neural networks, recurrent models, and reinforcement learning were applied to sensor fusion datasets combining LiDAR, radar, and GPS signals. Models were evaluated on their ability to detect adversarial spoofing attacks.
4. **Integration Simulation**: A simulated smart highway with 5,000 autonomous vehicles was built. Blockchain logged all communication events. AI monitored sensor data and network traffic for anomalies. Outcomes were measured in detection rate, system latency, and accident avoidance.

This methodology captured both the technical feasibility and operational challenges of blockchain-AI threat intelligence in transportation.

Current Standing

Autonomous vehicles remain at early stages of adoption, but security concerns are already visible. Researchers have demonstrated remote hijacking of connected cars through weak APIs. GPS spoofing has misled autonomous navigation. Smart traffic systems have been manipulated to disrupt flow. These incidents show that cyberattacks on transport can cause immediate physical consequences.

Blockchain improves security by decentralizing trust in V2V and V2I communication. Vehicles can use blockchain-based identity to verify each other before exchanging data. Immutable logs also provide forensic evidence in case of disputes. In pilots, blockchain reduced false communication signals in vehicle networks by over 60 percent. Still, blockchain faces scalability limits. Current frameworks struggle to process the millions of messages per second required on busy highways. Latency also poses risks, as authentication must happen within milliseconds to ensure safety.

AI strengthens monitoring by detecting abnormal patterns in vehicle behavior and communication. Machine learning models can flag spoofed GPS signals, abnormal braking patterns, or malicious V2V messages. For example, deep learning models applied to LiDAR datasets identified spoofed signals with precision above 90 percent in test environments. Yet AI faces challenges of adversarial manipulation. Attackers have shown that small changes to traffic signs can fool recognition systems. False positives remain a problem, as unnecessary interventions could disrupt traffic safety.

Commercial adoption is cautious. Automakers recognize the need for cybersecurity but face liability concerns. Regulators have yet to define clear standards for blockchain or AI in autonomous transport. As a result, blockchain-AI deployments remain limited to pilots in Japan, Germany, and the U.S.

Future Outlook

The next decade will see rapid expansion of autonomous transportation, making blockchain and AI threat intelligence essential.

1. **Blockchain Identity Chips**: By 2030, autonomous vehicles will include blockchain-enabled chips that generate cryptographic keys for all communication. These chips will ensure that only verified vehicles and infrastructure exchange data.

2. **Real-Time AI Threat Detection**: AI will evolve from anomaly detection to full predictive defense. Models will learn normal traffic patterns across cities and identify emerging threats in real time. Edge deployment will allow vehicles to run lightweight models locally, reducing latency.
3. **Consortium Blockchains**: Transportation authorities, automakers, and telecoms will form blockchain consortiums to manage V2V and V2I trust frameworks. This will replace proprietary systems with shared, standardized platforms. Immutable logs will also support liability resolution in accidents.
4. **Integration with 5G/6G Networks**: High-speed networks will enable low-latency blockchain-AI integration. Vehicles will communicate millions of events per second while maintaining secure authentication. By 2035, 6G-enabled blockchain ledgers are projected to handle global transport transactions in real time.
5. **Regulation and Compliance**: Governments will enforce blockchain-backed auditability and AI monitoring for autonomous transport systems. In the U.S., the Department of Transportation and NHTSA may require blockchain event logging for liability. The EU will likely adopt similar rules under transport cybersecurity regulations.
6. **Threat Intelligence Sharing**: National agencies will collaborate through blockchain-backed registries of vehicle threat intelligence. AI models will train on shared global data, improving resilience against new attacks.

The long-term outlook is an autonomous transportation system that is not only smart but also self-defending. Blockchain ensures trust in every communication, while AI prevents attacks from escalating into accidents.

Closing Remarks

Autonomous transportation depends on trust. Blockchain provides that trust through decentralized authentication and immutable records. AI adds intelligence through anomaly detection and predictive defense. Together, they form the foundation of safe and resilient autonomous mobility. Technical and regulatory barriers remain, but the trajectory is clear. By 2035, blockchain-AI threat intelligence will be mandatory in transportation networks, ensuring safety, accountability, and public confidence in self-driving systems.

References

- Mirza, J. B., Hasan, M. M., Paul, R., Hasan, M. R., & Asha, A. I. (2025). AI-Driven Business Intelligence in Retail: Transforming Customer Data into Strategic Decision-Making Tools. AIJMR-Advanced International Journal of Multidisciplinary Research, 3(1).

- Hasan, M. R., Hasan, M. M., Mirza, J. B., Hassan, A., Paul, R., Khan, M. N., & Nikita, N. A. (2025). The Role of AI in Digital Marketing Analytics: Enhancing Customer Segmentation and Personalization in IT Service-Based Businesses. AIJMR-Advanced International Journal of Multidisciplinary Research, 3(1).

- Arafat, M. S., Mirza, J. B., Jony, M. A. M., Islam, R., Rafi, S. S., Jalil, M. S., & Hossen, F. (2024). Blockchain and IoT Integration for Secure Supply Chain Operations: Unlocking Real-Time Transparency and Business Continuity. AIJMR-Advanced International Journal of Multidisciplinary Research, 2(6).

- Hassan, A., Hasan, M. M., Mirza, J. B., Paul, R., & Hasan, M. R. (2025). Optimizing IT Service Delivery with AI-Powered Digital Marketing Analytics: Understanding Client Needs for Enhanced Support Solutions. AIJMR-Advanced International Journal of Multidisciplinary Research, 3(1).